



STORMSHIELD



GUIDE

**STORMSHIELD NETWORK SSL VPN
CLIENT**

GUIDE D'INSTALLATION

Version 5.1.1 EA

Dernière mise à jour du document : 22 juillet 2025

Référence : sns-fr-ssl_vpn_client_guide_installation-v5.1.1-EA



Table des matières

Historique des modifications	3
Avant de commencer	4
Spécificités du client VPN SSL Stormshield	5
Versions et systèmes d'exploitation compatibles	5
Modes de connexion	5
Ports et protocoles	5
Exécution de scripts	6
Limitations et précisions sur les cas d'utilisation	6
Installation sur le système d'exploitation Windows	7
Télécharger le programme d'installation pour Windows	7
Installer le client VPN SSL Stormshield	7
Installation manuelle avec le package MSI	7
Déploiement via une stratégie de groupe (GPO)	8
Déploiement via un script	9
Mettre à jour le client VPN SSL Stormshield	9
Matrice de mise à jour vers une version 5	9
Mise à jour manuelle avec le package MSI	10
Déploiement de la mise à jour via une stratégie de groupe (GPO)	10
Déploiement de la mise à jour via un script	11
Désinstaller le client VPN SSL Stormshield	11
Installation sur le système d'exploitation Linux	13
Télécharger le programme d'installation pour Linux	13
Installer le client VPN SSL Stormshield	13
Installation sous Ubuntu	13
Installation sous RHEL	14
Désinstaller le client VPN SSL Stormshield	15
Désinstallation sous Ubuntu	15
Désinstallation sous RHEL	15
Installation sur le système d'exploitation macOS	16
Télécharger le programme d'installation pour macOS	16
Installer le client VPN SSL Stormshield	16
Désinstaller le client VPN SSL Stormshield	17
Pour aller plus loin	18



Historique des modifications

Date	Description
22 juillet 2025	Nouveau document



Avant de commencer

Bienvenue dans le guide d'installation de Stormshield Network SSL VPN Client version 5.1.1 EA.

Ce guide explique comment installer, mettre à jour et désinstaller le client VPN SSL Stormshield sur les systèmes d'exploitation Windows, Linux et macOS.

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée à des ressources, internes à une organisation ou non, en passant par le firewall SNS. Pour établir une connexion VPN SSL avec le firewall SNS, un client VPN SSL, comme le client VPN SSL Stormshield, doit être installé sur le poste de travail de chaque utilisateur.

Dans ce guide, Stormshield Network SSL VPN Client est nommé "client VPN SSL Stormshield".



Spécificités du client VPN SSL Stormshield

Cette section présente certaines spécificités du client VPN SSL Stormshield.

Versions et systèmes d'exploitation compatibles

Pour plus d'informations sur les systèmes d'exploitation et les versions compatibles, reportez-vous à la section [VPN SSL Client](#) du document *Cycle de vie produits Network Security & Tools*.

Modes de connexion

Mode de connexion	Description
Mode Stormshield	Ce mode doit être utilisé avec un firewall SNS Stormshield. Avec ce mode : <ul style="list-style-type: none">Le client VPN SSL Stormshield récupère automatiquement la configuration VPN SSL lors de la première connexion au firewall SNS ou lors des connexions suivantes si la configuration VPN SSL a été modifiée. Le client VPN SSL Stormshield vérifie à chaque connexion sur le firewall SNS si la configuration VPN SSL locale de la connexion utilisée doit être mise à jour.Le client VPN SSL Stormshield transmet au firewall SNS à chaque connexion les informations permettant de vérifier la conformité du poste client (ZTNA).
Import de fichier OVPN	Ce mode permet d'importer un fichier de configuration OpenVPN (format OVPN), et de se connecter à la passerelle OpenVPN ayant fourni le fichier de configuration.

Ports et protocoles

Dans une configuration par défaut, le client VPN SSL Stormshield doit pouvoir joindre les ports suivants pour établir des connexions VPN SSL.

Source	Destination	Protocole / Port (par défaut)	Objectif de la connexion
Client (SSLVPNService) Mode Stormshield uniquement	Passerelle OpenVPN	TCP/443 (portail captif)	Récupération de la configuration VPN SSL et envoi au firewall SNS des informations pour vérifier la conformité du poste client utilisé (ZTNA).
Client (OpenVPN)	Passerelle OpenVPN	UDP/1194 (VPN SSL)	Établissement d'une connexion VPN SSL
Client (OpenVPN)	Passerelle OpenVPN	TCP/443 (VPN SSL)	Établissement d'une connexion VPN SSL (Compatibilité)

Pour établir une connexion VPN SSL, le client VPN SSL Stormshield choisit toujours en premier le réseau UDP pour de meilleures performances.



Exécution de scripts

Le client VPN SSL Stormshield peut exécuter automatiquement des scripts sur le poste de travail de l'utilisateur à chaque ouverture et fermeture d'une connexion VPN SSL.

Système d'exploitation	Fonctionnement / Mise en place
Windows	Les scripts à exécuter doivent être ajoutés dans la configuration du service VPN SSL du firewall SNS.
Linux	Vous devez ajouter les scripts sslvpn_connect.sh et sslvpn_disconnect.sh sur chaque poste de travail à cet emplacement : <code>/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/</code>
macOS	Vous devez ajouter les scripts sslvpn_connect.sh et sslvpn_disconnect.sh sur chaque poste de travail à cet emplacement : <code>/Applications/Stormshield/SSL VPN Client.app/Contents/MacOS/Modules/ssl-vpn/etc/</code>

Sur les environnements Linux et macOS, vous devez respecter l'emplacement et le nom des scripts mentionnés ci-dessus.

Limitations et précisions sur les cas d'utilisation

Pour plus d'informations, reportez-vous à la section [Limitations et précisions sur les cas d'utilisation](#) des *Notes de Version SSL VPN Client*.



Installation sur le système d'exploitation Windows

Cette section explique comment installer, mettre à jour et désinstaller le client VPN SSL Stormshield sur le système d'exploitation Windows.

Télécharger le programme d'installation pour Windows

1. Vous pouvez télécharger le package MSI du client VPN SSL Stormshield depuis :
 - Le site Stormshield VPN SSL à l'adresse <https://vpn.stormshield.eu/>,
 - Votre **espace MyStormshield** dans **Téléchargements > Téléchargements > Stormshield Network Security > VPN SSL**.

Deux packages MSI sont disponibles : un en français et le second en anglais. Seule la langue du programme d'installation est différente. Une fois installé, le client VPN SSL Stormshield peut être utilisé en français ou en anglais.

2. Vérifiez l'intégrité du fichier téléchargé :
 - a. Dans l'invite de commandes Windows, récupérez l'empreinte du package MSI avec la commande :

```
CertUtil -hashfile <filename> SHA256
```

Remplacez *<filename>* par le nom du package MSI téléchargé.
 - b. Comparez le résultat obtenu avec l'empreinte visible depuis :
 - Le site **Stormshield VPN SSL**, bouton **GPG Signature**,
 - Votre **espace MyStormshield**, colonne **SHA256** du tableau des téléchargements.Les empreintes doivent être identiques.

Installer le client VPN SSL Stormshield

Vous pouvez installer le client VPN SSL Stormshield selon les méthodes suivantes :

- Installation manuelle avec le package MSI,
- Déploiement via une stratégie de groupe (GPO),
- Déploiement via un script.

i NOTE

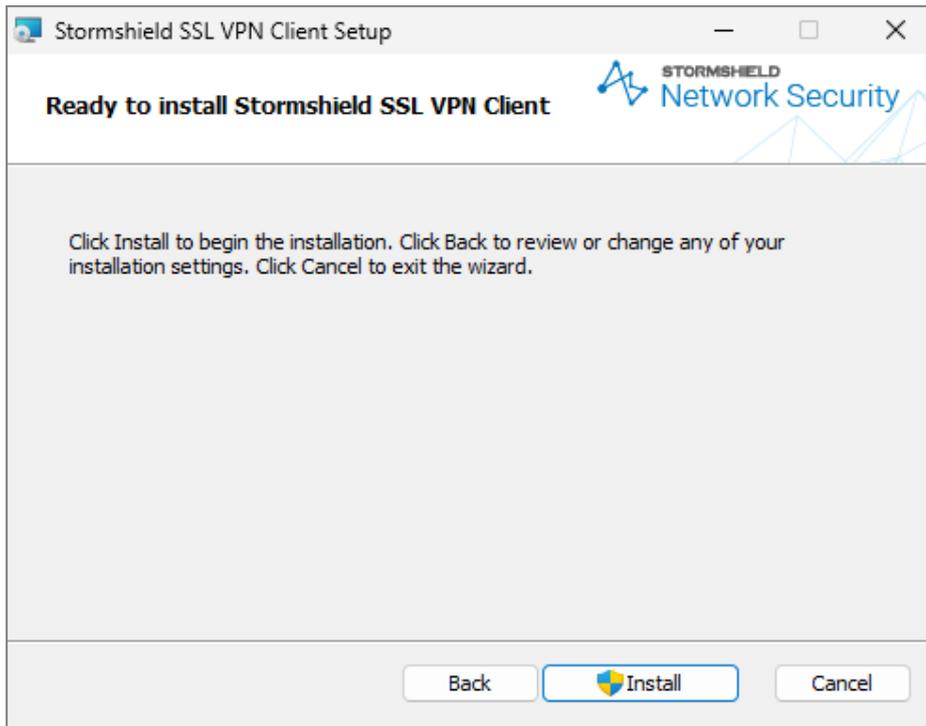
Lorsque vous installez le client VPN SSL Stormshield, il est installé pour tous les utilisateurs du poste de travail.

Installation manuelle avec le package MSI

Vous devez être administrateur local du poste de travail ou fournir le nom et le mot de passe d'un compte administrateur pour installer le client VPN SSL Stormshield.



1. Exécutez le package MSI [téléchargé préalablement](#).
2. Suivez les étapes de l'assistant d'installation.



Une fois installé, le client VPN SSL Stormshield démarre automatiquement.

Déploiement via une stratégie de groupe (GPO)

1. Sur le contrôleur de domaine, lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils > Gestion des stratégies de groupe**.
3. Dans la liste de gauche, effectuez un clic droit sur le nom du domaine Microsoft Active Directory et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici...**
4. Nommez la GPO et cliquez sur **OK**.
5. Effectuez un clic droit sur le nom de la GPO que vous venez de créer et sélectionnez **Modifier**.
6. Dans la fenêtre d'édition de la GPO, déployez à gauche le menu **Configuration ordinateur > Stratégies > Paramètres du logiciel**.
7. Effectuez un clic droit sur **Installation de logiciel** et sélectionnez **Nouveau > Package**. Sélectionnez le package MSI [téléchargé préalablement](#).
8. Choisissez le type de déploiement **Avancé** et cliquez sur **OK**.
9. Effectuez un clic droit sur le package que vous venez d'ajouter et sélectionnez **Propriétés**.
10. Dans l'onglet **Général**, vous pouvez renommer cette instance d'installation du package si vous le souhaitez.
11. Dans l'onglet **Déploiement**, cliquez sur **Options avancées...** et cochez **Ignorer la langue lors du déploiement de ce paquet**. Cliquez sur **OK**.
12. Cliquez sur **OK**.

Le déploiement est automatique lorsqu'un poste de travail se connecte au réseau de l'organisation. Une fois déployé, le client VPN SSL Stormshield démarre automatiquement.



Déploiement via un script

1. Ouvrez l'invite de commandes Windows en tant qu'administrateur.
2. Allez dans le dossier où se trouve le package MSI [téléchargé préalablement](#).
3. Exécutez cette commande pour débiter le déploiement :

```
msiexec /i <filename> /qn
```

- Remplacez *<filename>* par le nom du package MSI téléchargé.
- Conservez les options **/qn** pour que le déploiement s'effectue silencieusement sans afficher de barre de progression. Utilisez les options **/qb!** pour afficher une barre de progression.

Une fois déployé, le client VPN SSL Stormshield démarre automatiquement.

Mettre à jour le client VPN SSL Stormshield

Vous pouvez mettre à jour le client VPN SSL Stormshield selon les méthodes suivantes :

- Mise à jour manuelle avec le package MSI,
- Déploiement de la mise à jour via une stratégie de groupe (GPO),
- Déploiement de la mise à jour via un script.

Matrice de mise à jour vers une version 5

Version d'origine	Informations à prendre en compte dans le cas d'une mise à jour vers une version 5
Version 2 Version 3	<ul style="list-style-type: none">❌ Désinstallation obligatoire de la version d'origine avant de mettre à jour✅ Entrées du carnet d'adresses ajoutées dans les connexions enregistrées (*)❌ Profils de connexion importés (fichiers .ovpn) perdus
Version 4	<ul style="list-style-type: none">✅ Mise à jour possible sans désinstaller la version d'origine✅ Entrées du carnet d'adresses ajoutées dans les connexions enregistrées (*)❌ Profils de connexion importés (fichiers .ovpn) perdus
Version 5	<ul style="list-style-type: none">✅ Mise à jour possible sans désinstaller la version d'origine✅ Connexions enregistrées conservées

(*) À partir de la version 5, le "Carnet d'adresses" est intitulé "Connexions enregistrées". Lors d'une mise à jour depuis une version 4 ou inférieure vers une version 5, les entrées du carnet d'adresses sont ajoutées aux connexions enregistrées, soit automatiquement, soit en renseignant au premier démarrage du client VPN SSL Stormshield le mot de passe du carnet d'adresses si ce dernier est protégé. Le carnet d'adresses d'origine n'est pas modifié et est conservé à son emplacement d'origine.

! IMPORTANT

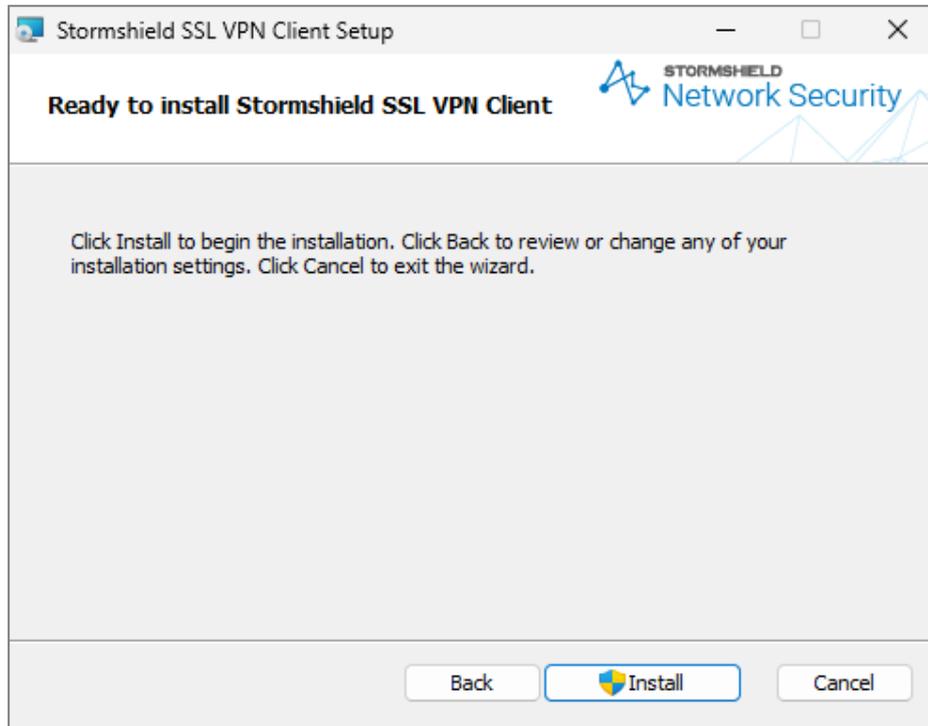
Le retour à une version inférieure à la version 5 n'est pas supporté. Si vous souhaitez tout de même revenir à la version 4 du client VPN SSL Stormshield, vous devez d'abord désinstaller la version 5, puis installer la version 4.



Mise à jour manuelle avec le package MSI

Vous devez être administrateur local du poste de travail ou fournir le nom et le mot de passe d'un compte administrateur pour installer la mise à jour du client VPN SSL Stormshield.

1. Exécutez le package MSI de la nouvelle version [téléchargé préalablement](#).
2. Suivez les étapes de l'assistant d'installation.



Une fois installé, le client VPN SSL Stormshield démarre automatiquement.

Déploiement de la mise à jour via une stratégie de groupe (GPO)

1. Sur le contrôleur de domaine, lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils > Gestion des stratégies de groupe**.
3. Dans la liste de gauche, effectuez un clic droit sur le nom de la GPO concernée et sélectionnez **Modifier**.
4. Dans la fenêtre d'édition de la GPO, déployez à gauche le menu **Configuration ordinateur > Stratégies > Paramètres du logiciel**.
5. Effectuez un clic droit sur **Installation de logiciel** et sélectionnez **Nouveau > Package**. Sélectionnez le nouveau package MSI [téléchargé préalablement](#).
6. Choisissez le mode **Avancé** et cliquez sur **OK**.
7. Effectuez un clic droit sur le package que vous venez d'ajouter et sélectionnez **Propriétés**.
8. Dans l'onglet **Général**, renommez cette instance d'installation si vous le souhaitez en y ajoutant par exemple le numéro de version du client VPN SSL Stormshield.
9. Dans l'onglet **Déploiement**, cliquez sur **Options avancées...** et cochez **Ignorer la langue lors du déploiement de ce paquet**. Cliquez sur **OK**.



10. Dans l'onglet **Mises à niveau** :
 - a. L'instance d'installation du précédent package est affichée avec la mention **Mettre à niveau**. Sélectionnez-la et cliquez sur **Supprimer**. Vous devez modifier cette propriété pour que la mise à jour s'effectue correctement.
 - b. Cliquez sur **Ajouter...**, sélectionnez le package de mise à jour et cochez **Désinstaller le package existant, puis installer le package de mise à niveau**. Cliquez sur **OK**.
L'instance d'installation du précédent package est désormais associée à l'action **Remplacer**.
11. Cliquez sur **OK**.
Le package de mise à jour est désormais prêt à être déployé. Le déploiement est automatique lorsqu'un poste de travail se connecte au réseau de l'organisation. Une fois la mise à jour déployée, le client VPN SSL Stormshield démarre automatiquement.

Déploiement de la mise à jour via un script

1. Ouvrez l'invite de commandes Windows en tant qu'administrateur.
2. Allez dans le dossier où se trouve le package MSI **téléchargé préalablement**.
3. Exécutez cette commande pour débiter la mise à jour :

```
msiexec /i <filename> /qn
```

- Remplacez *<filename>* par le nom du package MSI téléchargé.
- Conservez les options **/qn** pour que le déploiement s'effectue silencieusement sans afficher de barre de progression. Utilisez les options **/qb!** pour afficher une barre de progression.

Une fois la mise à jour déployée, le client VPN SSL Stormshield démarre automatiquement.

Désinstaller le client VPN SSL Stormshield

Vous devez être administrateur local du poste de travail ou fournir le nom et le mot de passe d'un compte administrateur pour désinstaller le client VPN SSL Stormshield.

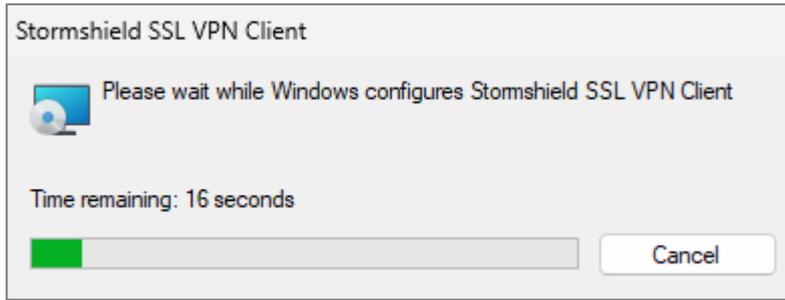
i NOTE

Certains fichiers persistent après la désinstallation du client VPN SSL Stormshield, comme les fichiers de logs et le fichier .book contenant les connexions enregistrées.

1. Assurez-vous que le client VPN SSL Stormshield ne soit plus en cours d'exécution.
2. Rendez-vous dans le menu **Démarrer** de Windows et ouvrez les **Paramètres**.
3. Sous Windows 11, rendez-vous dans **Applications > Applications installées**.
Sous Windows 10, rendez-vous dans **Applications > Applications et fonctionnalités**.
4. Sous Windows 11, repérez **Stormshield SSL VPN Client** et cliquez sur **... > Désinstaller**.
Sous Windows 10, sélectionnez **Stormshield SSL VPN Client** et cliquez sur **Désinstaller**.
5. Cliquez une nouvelle fois sur **Désinstaller** pour démarrer la désinstallation.



6. Patientez pendant que le client VPN SSL Stormshield se désinstalle.



Le client VPN SSL Stormshield est désinstallé pour tous les utilisateurs du poste de travail.



Installation sur le système d'exploitation Linux

Cette section explique comment installer et désinstaller le client VPN SSL Stormshield sur le système d'exploitation Linux.

Télécharger le programme d'installation pour Linux

1. Vous pouvez télécharger le paquet d'installation du client VPN SSL Stormshield depuis :
 - Le site Stormshield VPN SSL à l'adresse <https://vpn.stormshield.eu/>,
 - Votre [espace MyStormshield](#) dans **Téléchargements > Téléchargements > Stormshield Network Security > VPN SSL**.

Le paquet d'installation est disponible au format .deb pour les distributions Ubuntu et au format .rpm pour les distributions RHEL.

2. Vérifiez l'intégrité du fichier téléchargé :
 - a. Dans un terminal, récupérez l'empreinte du paquet d'installation avec la commande :

```
sha256sum <filename>
```

Remplacez *<filename>* par le nom du paquet d'installation .deb ou .rpm téléchargé.
 - b. Comparez le résultat obtenu avec l'empreinte visible depuis :
 - Le site [Stormshield VPN SSL](#), bouton **GPG Signature**,
 - Votre [espace MyStormshield](#), colonne **SHA256** du tableau des téléchargements.Les empreintes doivent être identiques.

Installer le client VPN SSL Stormshield

NOTE

Ce section explique comment installer le client VPN SSL Stormshield pour Linux en ligne de commande.

Poursuivez selon la distribution Linux concernée.

Installation sous Ubuntu

1. Installez le client VPN SSL Stormshield :

```
sudo apt install ./<filename>
```

 - Remplacez *<filename>* par le nom du paquet .deb **téléchargé préalablement**.
 - Avec l'outil *apt*, vous devez fournir le chemin de fichier du paquet à installer. Dans l'exemple, */* indique que le paquet est disponible dans le répertoire courant.
2. Avec l'environnement de bureau par défaut, l'icône  du client VPN SSL Stormshield apparaît automatiquement dans la barre d'état système.

Si vous avez modifié la configuration de l'environnement de bureau ou si vous en utilisez un autre, assurez-vous d'afficher l'icône du client VPN SSL Stormshield dans la barre d'état système, par exemple en activant des options dans la configuration de l'environnement de bureau utilisé ou en installant un paquet supplémentaire.



3. Si votre passerelle OpenVPN (le firewall SNS) fournit une configuration DNS spécifique à utiliser, cette dernière n'est pas prise en compte nativement par OpenVPN sous Linux. Vous devez alors disposer localement d'une solution permettant de la prendre en compte. Par exemple, si vous utilisez le gestionnaire de résolution DNS par défaut *systemd-resolved* :
 - a. Installez le paquet **openvpn-systemd-resolved** :

```
sudo apt install openvpn-systemd-resolved
```
 - b. Créez des liens symboliques pour que le script contenu dans ce paquet soit utilisé par le client VPN SSL Stormshield à l'ouverture et à la fermeture d'une connexion VPN SSL. Respectez les emplacements et les noms spécifiés dans les commandes ci-dessous.

```
sudo ln -s /etc/openvpn/update-systemd-resolved /opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh
sudo ln -s /etc/openvpn/update-systemd-resolved /opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

Installation sous RHEL

1. Ajoutez manuellement un dépôt pour fournir la dépendance **openvpn**, qui n'est pas disponible par défaut sous RHEL. Vous pouvez par exemple ajouter le dépôt EPEL (**Extra Packages for Enterprise Linux**) :

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
sudo dnf update -y
```
2. Installez le client VPN SSL Stormshield :

```
sudo dnf install ./<filename>
```

 - Remplacez *<filename>* par le nom du paquet .rpm **téléchargé préalablement**.
 - Avec l'outil *dnf*, vous devez fournir le chemin de fichier du paquet à installer. Dans l'exemple, */* indique que le paquet est disponible dans le répertoire courant.
3. Avec l'environnement de bureau par défaut, vous devez installer un paquet permettant de faire apparaître l'icône  du client VPN SSL Stormshield dans la barre d'état système, comme le paquet **gnome-shell-extension-appindicator**. Si vous en utilisez un autre, assurez-vous d'afficher l'icône du client VPN SSL Stormshield dans la barre d'état système.
4. Si votre passerelle OpenVPN (le firewall SNS) fournit une configuration DNS spécifique à utiliser, cette dernière n'est pas prise en compte nativement par OpenVPN sous Linux. Vous devez alors disposer localement d'une solution permettant de la prendre en compte. Vous pouvez par exemple utiliser un script équivalent à celui du paquet **openvpn-systemd-resolved** sous Ubuntu.

Une fois le script en votre possession, vous devez créer des liens symboliques pour que ce script soit utilisé par le client VPN SSL Stormshield à l'ouverture et à la fermeture d'une connexion VPN SSL. Les scripts du client VPN SSL Stormshield doivent se trouver à l'emplacement ci-dessous et être nommés de la manière suivante :

```
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_connect.sh
/opt/stormshield/sslvpnclient/modules/ssl-vpn/etc/sslvpn_disconnect.sh
```



Désinstaller le client VPN SSL Stormshield

i NOTE

Certains fichiers persistent après la désinstallation du client VPN SSL Stormshield, comme les fichiers de logs et le fichier .book contenant les connexions enregistrées.

Désinstallation sous Ubuntu

1. Assurez-vous que le client VPN SSL Stormshield ne soit plus en cours d'exécution.
2. Désinstallez le client VPN SSL Stormshield :

```
sudo apt remove sslvpnclient
```

Désinstallation sous RHEL

1. Assurez-vous que le client VPN SSL Stormshield ne soit plus en cours d'exécution.
2. Désinstallez le client VPN SSL Stormshield :

```
sudo dnf remove sslvpnclient
```



Installation sur le système d'exploitation macOS

Cette section explique comment installer et désinstaller le client VPN SSL Stormshield sur le système d'exploitation macOS.

Télécharger le programme d'installation pour macOS

1. Vous pouvez télécharger le paquet d'installation (fichier .pkg) du client VPN SSL Stormshield depuis :
 - Le site Stormshield VPN SSL à l'adresse <https://vpn.stormshield.eu/>,
 - Votre [espace MyStormshield](#) dans **Téléchargements > Téléchargements > Stormshield Network Security > VPN SSL**.
2. Vérifiez l'intégrité du fichier téléchargé :
 - a. Dans un terminal, récupérez l'empreinte du paquet d'installation avec la commande :

```
shasum -a 256 <filename>
```

Remplacez *<filename>* par le nom du fichier .pkg téléchargé .
 - b. Comparez le résultat obtenu avec l'empreinte visible depuis :
 - Le site [Stormshield VPN SSL](#), bouton **GPG Signature**,
 - Votre [espace MyStormshield](#), colonne **SHA256** du tableau des téléchargements.Les empreintes doivent être identiques.

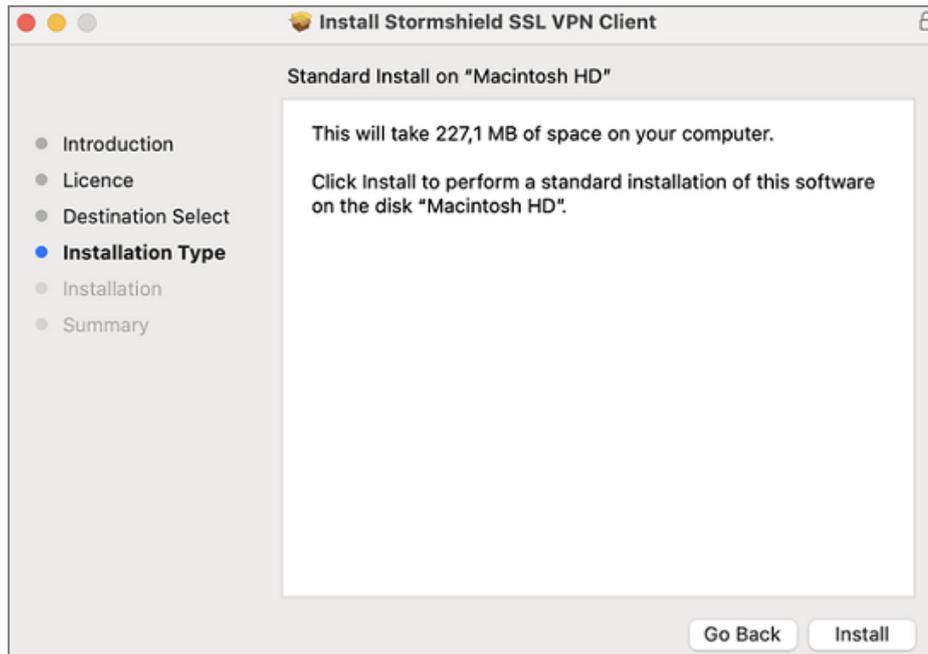
Installer le client VPN SSL Stormshield

Vous pouvez installer le client VPN SSL Stormshield, soit manuellement en exécutant le paquet d'installation .pkg, soit en utilisant une solution de gestion des appareils mobiles (MDM). Dans cette section, seule la procédure d'installation manuelle est expliquée.

Vous devez être administrateur local du poste de travail pour installer le client VPN SSL Stormshield.



1. Exécutez le paquet d'installation (fichier .pkg) [téléchargé préalablement](#).
2. Suivez les étapes de l'assistant d'installation.



3. Si votre passerelle OpenVPN (le firewall SNS) fournit une configuration DNS spécifique à utiliser, cette dernière n'est pas prise en compte nativement par OpenVPN sous macOS. Vous devez alors disposer localement d'une solution permettant de la prendre en compte, comme utiliser un script tiers.

Une fois le script en votre possession, vous devez créer des liens symboliques pour que ce script soit utilisé par le client VPN SSL Stormshield à l'ouverture et à la fermeture d'une connexion VPN SSL. Les scripts du client VPN SSL Stormshield doivent se trouver à l'emplacement ci-dessous et être nommés de la manière suivante :

```
/Applications/Stormshield/SSL VPN Client.app/Contents/MacOS/Modules/ssl-vpn/etc/sslvpn_connect.sh  
/Applications/Stormshield/SSL VPN Client.app/Contents/MacOS/Modules/ssl-vpn/etc/sslvpn_disconnect.sh
```

Désinstaller le client VPN SSL Stormshield

Vous devez être administrateur local du poste de travail pour désinstaller le client VPN SSL Stormshield.

i NOTE

Certains fichiers persistent après la désinstallation du client VPN SSL Stormshield, comme les fichiers de logs et le fichier .book contenant les connexions enregistrées.

1. Assurez-vous que le client VPN SSL Stormshield ne soit plus en cours d'exécution.
2. Accédez au **Finder**, et rendez-vous dans le dossier **Applications**.
3. Effectuez un clic droit sur l'icône du client VPN SSL Stormshield, et cliquez sur **Placer dans la corbeille**.
4. Videz la corbeille pour supprimer l'application.



Pour aller plus loin

Pour configurer le service VPN SSL du firewall SNS, reportez-vous à la section [VPN SSL](#) du *Manuel Utilisateur SNS* de la version utilisée.

Des informations complémentaires et réponses à vos éventuelles questions sur le client VPN SSL Stormshield sont disponibles dans la [base de connaissances Stormshield](#) [authentification nécessaire].



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.